BB

PATENT ABSTRACTS OF JAPAN

(11)Publication numb r : 11-212922
(43)Date of publication of application : 06.08.1999

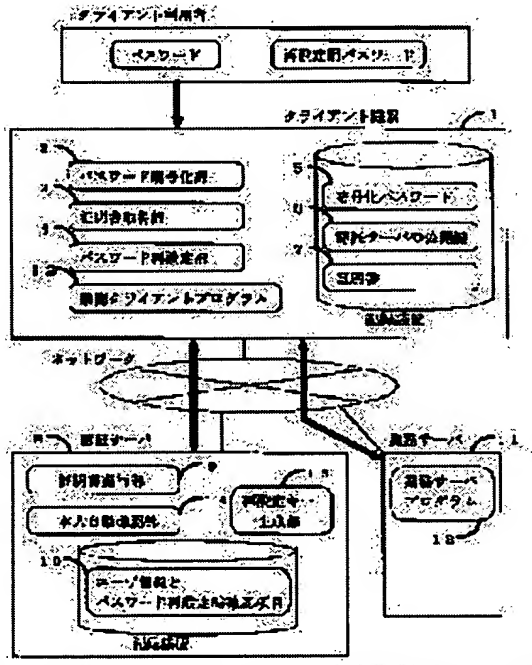
(51)Int.Cl. G06F 15/00

(21)Application number : 10-010141
(22)Date of filing : 22.01.1998

(71)Applicant : HITACHI LTD
(72)Inventor : OCHI YASUSHI

(54) PASSWORD MANAGEMENT AND RECOVERY SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable a user to safely set a password again without danger by transmitting an inquiry code to a server and producing a key for password setting when the user forgets the password.
SOLUTION: When a client user forgets his password, a password for resetting is inputted to a password resetting part 4 on a client device 1, an inquiry code is produced and it is sent together with a user identifier to an authentication server 8. When the part 4 sends the inquiry code to the server 8 and when an automatic person himself/herself confirming part 14 recognizes that input information is legal from user information and confirmation items 10 at the time of resetting a password, a resetting key generating part 15 produces a resetting key from the inquiry code and returns it to the device 1. The part 4 which receives the resetting key authenticates the validity from the combination of an encipher password 5 and the resetting key and allows the user to set the password.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－212922

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｅ

審査請求　未請求　請求項の数２　ＯＬ　（全　５　頁）

(21)出願番号　特願平10－10141

(22)出願日　平成10年(1998)１月22日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

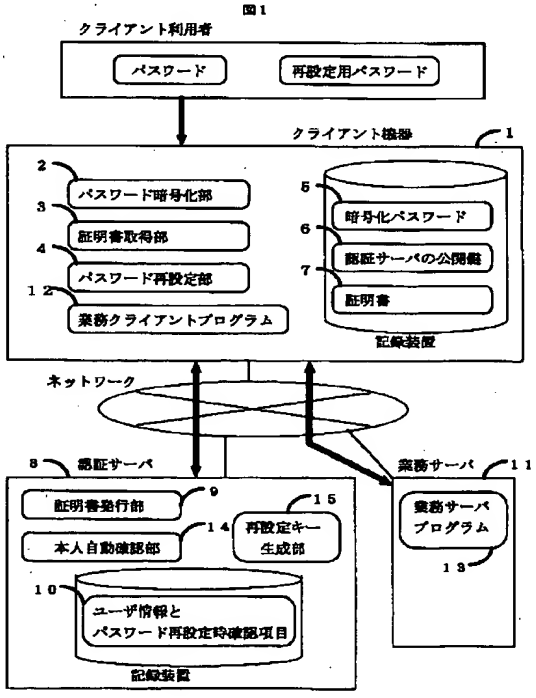
(72)発明者　越智　康
神奈川県横浜市戸塚区戸塚町5030番地株式会社日立製作所ソフトウェア開発本部内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　パスワード管理、回復方式

(57)【要約】
【課題】パスワードを忘れた場合でも、他者にパスワードを知られる危険無く、またクライアントアプリケーションの再初期設定無く、復旧することにある。
【解決手段】クライアント機器１は、パスワード再設定時に認証サーバ８と連携して、本人自動確認及び再設定キーを得る。クライアント機器１は再設定キーと暗号化されたパスワード５より利用者の正当性を確認し、パスワードの再設定を行う。

図１



1

【特許請求の範囲】
【請求項１】クライアント・サーバシステムにおいて、クライアント機器を使用するために、パスワードを用いて利用者を制限する方式において、
クライアント機器利用者のセキュリティ保護のために、クライアント機器に保存するパスワードをアプリケーション独自の方式で暗号化する手段を有し、
クライアント機器利用者が設定したパスワードを忘れてしまった場合を想定し、クライアント側アプリケーションとサーバ側アプリケーションが連携することにより、誰も元のパスワードを知りうること無く、また、クライアント機器上のアプリケーションを再初期化設定することなく、クライアント機器上でクライアント機器利用者が再度パスワードを設定することを可能とすることを特徴とするパスワード管理、回復方式。
【請求項２】クライアント・サーバシステムにおいて、クライアントからサーバへの要求時に、クライアント利用者が、クライアント機器上でのアプリケーションを設定時に登録した正当なユーザであることを、サーバ機器上で自動的に確認するために、サーバ機器がクライアント利用者に対して対話的に確認する項目を、サーバ機器上に登録しておくことを特徴とする本人確認法式。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】パスワード方式を用いて、機器利用者を制限することで、不正使用を防止するセキュリティ技術に関する。
【０００２】
【従来の技術】パスワード技術を用いたセキュリティ技術は多くの利用例があるが大きく次に分類される。
【０００３】一つには、クライアント利用者のパスワードをサーバアプリケーションが動作するサーバ機器あるいは、別のユーザ情報管理用サーバ機器内に保管する方式である。この場合、利用者がパスワードを忘れた場合に、サーバ側オペレータがサーバ側の情報を元にパスワードを利用者に通知したり、利用者に再設定を可能とする処置を行うのが一般的である。
【０００４】もう一つの方式として、クライアント利用者のパスワードをＰＣ等のクライアント機器内に保管する方式がある。この場合、保管されているパスワードが、クライアント機器独自の方式で暗号化がなされていると、利用者がパスワードを忘れた場合には利用者以外該当パスワードを知り得ないため、忘れたパスワードを再度利用することは不可能であり、当該アプリケーションを使用して再度初期の設定等を行う必要があった。
【０００５】他に、特開平５－１７３９７２号公報に記載された方式では、クライアント機器にパスワードを保管する際に、公開鍵暗号システムにより、サーバ機器の公開鍵で暗号化したパスワードを保管し、利用者がパスワードを忘れた場合には、サーバ管理者に依頼して、サーバでパスワードの復号を行い、忘れたパスワードを再度利用することができる。

2

【０００６】また、サーバへのパスワード通知または再設定の依頼に対して、依頼者が本人であることを確認するためには、サーバ側のアプリケーションが依頼者に対して一定の項目の入力を要求し、サーバ機器上のユーザ情報データベースと照合して確認する奉仕雨季がある。さらに確実に確認を行うには、オペレータ等の人手の介在が必要であった。
【０００７】
【発明が解決しようとする課題】上記従来技術のうち、サーバ機器にパスワードを保管する方式では、パスワードを忘れた利用者が、サーバ管理者にパスワードの通知を依頼した場合、サーバ管理者は容易に依頼者のパスワードを知りうることになる。パスワードの通知をネットワーク経由で行った場合は、通信路上でのパスワード漏洩への対策が別途必要になる。また、サーバ機器上にはすべてのユーザのパスワードが保管されているため、悪意あるサーバ管理者や、サーバ機器への不正侵入者がパスワードの不正取得を試みた場合の危険度が大きいという問題があった。
【０００８】また、クライアント機器に、クライアント独自の方式により暗号化されたパスワードを保管する方式では、パスワードを忘れた場合には、クライアント機器のアプリケーションを再初期設定しない限りクライアント機器が使用できないという問題があった。
【０００９】また、クライアント機器に、サーバの公開鍵で暗号化されたパスワードを保管する方式（特開平５－１７３９７２号公報）では、サーバ機器上にパスワードを保管する方式と同様に、パスワードを通知する際にサーバ管理者はパスワードを容易に知ることができる。通信路上での対策も同様に別途必要となる。
【００１０】また、パスワード通知または再設定依頼者が、本人であるかどうかを確認する際には、サーバ管理者などのオペレータによる人手の介在が必要であった。または、サーバ機器上のアプリケーションが、クライアント側の依頼者に対して一定の項目に対して対話的確認を行う方式では、利用者の氏名・所属等の他者が容易に知るうる情報が使用されることが多いため、不正使用に対するセキュリティが不十分であった。
【００１１】本発明の目的は上記の問題を解決することを目的とする。
【００１２】
【課題を解決するための手段】本発明によれば、クライアント利用者のパスワードをＰＣ等のクライアント機器内に保存する場あにも、利用者がパスワードを忘れた場合にも、そのパスワードをクライアント利用者以外に知られる危険性の無い安全な方式により、さらにアプリケーションの再初期設定を必要としない利便性を維持したまま、正当なクライアント機器利用者が再度当該機器を

使用するためにパスワード設定を可能とする。

【００１３】また、本発明によれば、パスワード再設定時に必要な、本人確認を安全かつ自動的に行うことを可能とする。

【００１４】上記目的を達成するため、請求項１に係るパスワード復旧・管理方式では、クライアント機器の正当な利用者以外の使用を制限するために、パスワードのよりクライアント機器の使用者を認証する。

【００１５】また、パスワードの漏洩を防ぐために、パスワードはクライアント機器上にしか保管せず、クライアント機器上に、クライアント利用者のパスワードを、クライアントごとに異なる情報（例えばクライアントのパスワード自身）を暗号鍵として暗号化されてクライアント機器内に保管する。

【００１６】また、クライアント利用者がパスワードを忘れた場合にクライアント機器上のアプリケーションの再初期設定を不要とするため、クライアント側機器にはパスワードを忘れた場合に、パスワード再設定を行うために投入する手段（コマンド等）を備える。このコマンドは、クライアント機器上で暗号化されたパスワード及びサーバとの連携のための秘密鍵により、問い合わせコード（例えば１０桁の１０進数）を出力する。次にクライアント利用者はこの問い合わせコードを、サーバ管理者に連絡する。次に、サーバ管理者は、問い合わせが本人であることを確認したのち、この問い合わせコードを利用してパスワード設定用のキーを生成する処理をサーバ機器で実行する。クライアント利用者は、サーバ管理者から通知されたキーをクライアント機器に投入することにより、クライアント機器はパスワード再設定を許可する。

【００１７】また、悪意あるサーバ管理者からのパスワード防御のために、サーバ側へ通知される問い合わせコードからは、パスワードは容易に復号できないように、クライアント機器上で暗号化されたパスワードを元に問い合わせコードを生成する。サーバ機器上にはクライアント機器のパスワードに関する情報は保管されていないため、不正侵入者の攻撃によりパスワードが漏洩する危険はない。また、通信路上でのパスワード漏洩または漏洩を防止するための対策について、通信路上にはクライアント機器上で暗号化されたパスワードを元にした情報しか流れないために、通信路上での漏洩の危険や漏洩防止のための対策は必要ない。

【００１８】なお、サーバ管理者がクライアント利用者を本人確認するために、電話により問診等を行うような、人が介在する方式が本人確認の手段として有効であるが、管理者の負担を軽減するためにサーバ機器があらかじめ登録された本人情報を対話的に問い合わせることにより自動的に本人確認する手段も可能である。

【００１９】上記の本人確認を安全かつ自動的に行う目的を達成するために、請求項２に係る本人確認法式では、クライアント利用者に対して、サーバから入力を求める項目を、クライアントがある程度自由に設定できるようにし、詐称した依頼者に対するセキュリティを高くしている。

【００２０】

【発明の実施の形態】以下、本発明の実施例を図１および図２により説明する。

【００２１】図１は、本発明のパスワード管理・回復方式を含む、認証サーバによってクライアントアプリケーションのアカウントを取得する、クライアントサーバシステムの構成例である。

【００２２】図２は、本発明のパスワード管理・回復方式における、本人確認法式に自動確認法式を採用した実施例での構成図である。

【００２３】クライアント機器の利用者を正当な利用者のみに限定するクライアントサーバシステムに適用する。

【００２４】特に、パスワードの新規設定が、認証サーバに対する証明書の再発行を必要とするようなパスワードを失うことの影響の大きなシステムを想定する。

【００２５】図１のクライアントサーバシステムでは、クライアント機器１上で業務クライアントプログラム１２により業務サーバプログラム１３へアクセスするためには、認証サーバ８より発行された証明書が必要である。クライアント機器上の業務クライアントプログラムを再初期設定すると、新たに証明書が必要となる。

【００２６】認証サーバ８で証明書を発行してもらう際に、クライアント利用者はユーザ情報と、パスワード再設定時の確認項目を設定し、この情報と認証サーバの公開鍵６を元に証明書取得部３は認証サーバにアクセスして証明書発行部９が発行する証明書を取得する。証明書７は認証サーバの公開鍵６と共にクライアント機器上に保管される。ユーザ情報とパスワード再設定時の確認項目１０は認証サーバ上に保管される。

【００２７】クライアント利用者は、クライアント機器１に対してパスワードを設定し、パスワードはクライアント機器上に、パスワード暗号化部２によって、クライアント機器独自の方式により暗号化されたパスワード５として保存される。この暗号化は、認証サーバを含む他の全てのシステムと独立であり、暗号化されたパスワード５が漏洩したとしても復号は困難である。

【００２８】クライアント利用者がパスワードを忘れた場合クライアント機器１上のパスワード再設定部４に対し、再設定依頼する認証サーバ用の再設定用パスワードを入力し、パスワード再設定部４により問い合わせコードを作成し、ユーザ識別子と共に認証サーバ８へ送信してパスワード再設定キーの返送を要求する。

【００２９】パスワード再設定部４は、認証サーバ８に問い合わせコードを送信する。認証サーバ８では、自動本人確認部１４がクライアント利用者に対して、予め設

5

定されたユーザ情報とパスワード再設定時の確認項目１０から、情報の入力を要請する。入力された情報が、照合の結果正当であると認められると、問い合わせコードから再設定キー生成部１５が再設定キー生成し、クライアント機器１に返送する。ここで、認証サーバ８はクライアント機器のパスワード暗号化方式を知らないため、容易に復号できない。

【００３０】再設定キーを受け取ったクライアント機器１のパスワード再設定部４では、暗号化されたパスワード５と再設定キーの組み合わせから、再設定キーの正当性を認証し、クライアント利用者に対してパスワードの再設定を許可する。

【００３１】上記の処理中に、コードの生成や照合が失敗すると、パスワードの再設定は行われない。

【００３２】また、再設定キー生成部１５は、ユーザ情報とパスワード再設定時の確認項目１０がアクセスできるシステムに存在すればよく、認証サーバ８、業務サーバ１１、または他のいかなるサーバ上にも存在できる。

【００３３】また、本人確認法式は、オペレータの電話等による問診による方式を採用することにより、さらに安全性を高めることができる。

【００３４】

【発明の効果】本発明は、以上に説明したように構成されているので、クライアント利用者が、本人の設定した

6

パスワードを忘れた場合にも当初のパスワード設定からやり直すこと無く、新たにパスワードを設定することを可能とする。

【００３５】さらに、他者（サーバ機器管理者やネットワーク盗聴者等）にパスワードを知られる危険が無く、この効果を実現することができる。

【図面の簡単な説明】

【図１】図１は、本発明のパスワード管理・回復方式を含む、認証サーバによってクライアントアプリケーションのアカウントを取得する、クライアントサーバシステムの構成例である。

【図２】図２は、本発明のパスワード管理・回復方式における、本人確認法式に自動確認法式を採用した実施例での構成図である。

【符号の説明】

１…クライアント機器、　２…パスワード暗号化部、３…証明書取得部、４…パスワード再設定部、５…暗号化されたパスワード、６…認証サーバの公開鍵、７…証明書、８…認証サーバ、９…証明書発行部、１０…ユーザ情報とパスワード再設定時確認項目、　１１…業務サーバ、１２…業務クライアントプログラム、　１３…業務サーバプログラム、１４…本人自動確認部、１５…再設定キー生成部。

【図１】

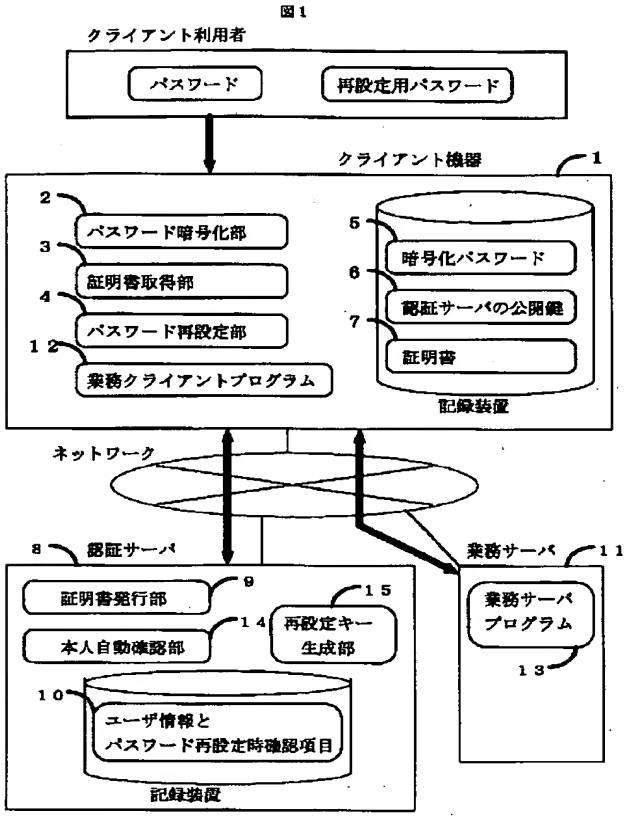


図1
クライアント利用者
パスワード
再設定用パスワード
クライアント機器
1
2
パスワード暗号化部
3
証明書取得部
4
パスワード再設定部
12
業務クライアントプログラム
5
暗号化パスワード
6
認証サーバの公開鍵
7
証明書
記録装置
ネットワーク
8
認証サーバ
証明書発行部
9
本人自動確認部
14
再設定キー生成部
15
10
ユーザ情報とパスワード再設定時確認項目
記録装置
業務サーバ
11
業務サーバプログラム
13

【図２】

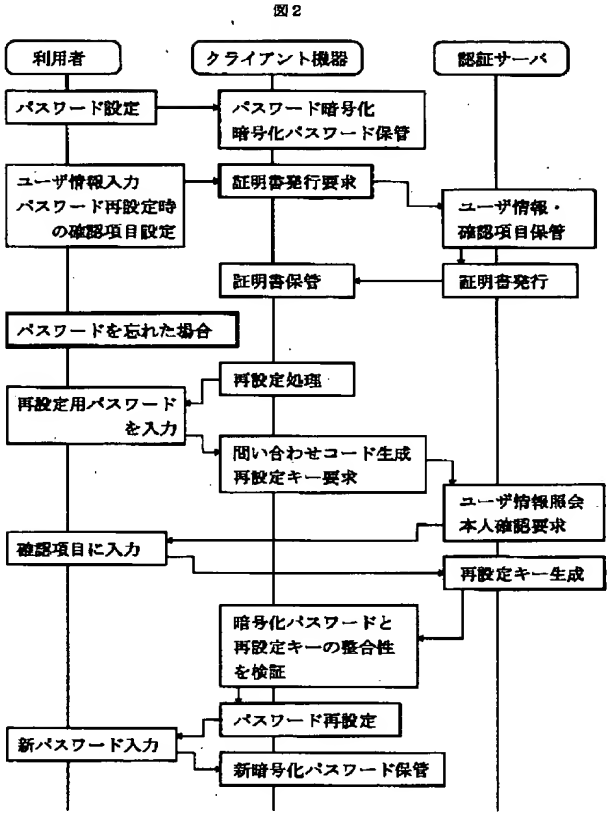


図2
利用者
クライアント機器
認証サーバ
パスワード設定
パスワード暗号化
暗号化パスワード保管
ユーザ情報入力
パスワード再設定時
の確認項目設定
証明書発行要求
ユーザ情報・
確認項目保管
証明書保管
証明書発行
パスワードを忘れた場合
再設定処理
再設定用パスワード
を入力
問い合わせコード生成
再設定キー要求
ユーザ情報照会
本人確認要求
確認項目に入力
再設定キー生成
暗号化パスワードと
再設定キーの整合性
を検証
パスワード再設定
新パスワード入力
新暗号化パスワード保管